

ELLIPTIC CURVES IN ISOGENY CLASSES

IGOR E. SHPARLINSKI AND LIANGYI ZHAO

ABSTRACT. We show that the distribution of elliptic curves in isogeny classes of curves with a given value of the Frobenius trace t becomes close to uniform even when t is averaged over very short intervals inside the Hasse-Weil interval.

1. INTRODUCTION

1.1. Motivation. Let $p > 3$ be prime and let E be an elliptic curve over the field \mathbb{F}_p of p elements given by an affine *Weierstrass equation* of the form

$$(1.1) \quad y^2 = x^3 + ax + b,$$

with coefficients $a, b \in \mathbb{F}_p$, such that $4a^3 + 27b^2 \neq 0$.

Clearly, there are $p^2 + O(p)$ suitable equations of the form (1.1). Furthermore, they generate $J = 2p + O(1)$ distinct (that is, non-isomorphic over \mathbb{F}_p) curves, and for most of the curves there are exactly $(p-1)/2$ distinct equations (1.1), see [6] for a discussion of these properties.

We recall that the cardinality of the set $E(\mathbb{F}_p)$ of \mathbb{F}_p -rational points on any elliptic curve E satisfies the *Hasse-Weil* bound which we formulate as

$$(1.2) \quad \#E(\mathbb{F}_p) - p - 1 \in [-T, T],$$

where

$$T = \lfloor 2p^{1/2} \rfloor,$$

we refer the reader to [7] for these and other general properties of elliptic curves.

Curves with the same value of $\#E(\mathbb{F}_p)$ are said to be isogenous. Hence, we see from (1.2) that there are $4p^{1/2} + O(1)$ isogeny classes.

Accordingly, we denote by $I(t)$ the number of distinct isomorphism classes in the isogeny class of curves with $\#E(\mathbb{F}_p) = p + 1 - t$, for

Date: November 17, 2016.

2010 Mathematics Subject Classification. 11G07, 11L40, 11N35.

Key words and phrases. Elliptic curves, isogeny classes, class number.

$t \in [-T, T]$. Clearly, the average value of $I(t)$ is

$$(1.3) \quad \begin{aligned} \frac{1}{2T+1} \sum_{-T \leq t \leq T} I(t) &= \frac{J}{2T+1} \\ &= \frac{2p + O(1)}{4p^{1/2} + O(1)} = 0.5p^{1/2} + O(1). \end{aligned}$$

Thus, on average, each isogeny class contains $0.5p^{1/2}$ isomorphic curves, which motivates the study of the distribution of the values

$$\iota(t) = \frac{I(t)}{0.5p^{1/2}}$$

Lenstra [6] has obtained upper and lower bounds for this number which show that typically the values of $I(t)$ are of the same order of magnitude as their average value. In particular, by [6, Proposition 1.9 (a)], for any $t \in [-2p^{1/2}, 2p^{1/2}]$ we have

$$(1.4) \quad \iota(t) = O\left(\log p (\log \log p)^2\right),$$

with an absolute implied constant. We see that the upper bound (1.4) contains some extra logarithmic factors compared to the average value 1, see (1.3)

On the other hand, the result of Birch [3] on the *Sato-Tate conjecture* over the family of all isomorphism classes of elliptic curves over \mathbb{F}_p implies the asymptotic formula (which is uniform over real $\alpha, \beta \in [-1, 1]$)

$$(1.5) \quad \sum_{\alpha T \leq t \leq \beta T} \iota(t) = \mu(\alpha, \beta)T + o(p),$$

where $\mu(\alpha, \beta)$ is the *Sato-Tate density* given by

$$\mu(\alpha, \beta) = \frac{2}{\pi} \int_{\arccos \alpha}^{\arccos \beta} \sin^2 \vartheta \, d\vartheta.$$

Here we obtain an upper bound which in some sense interpolates between (1.4) and (1.5) and improves (1.4) on average over t over rather short interval.

1.2. Notation. Throughout the paper, p always denotes a prime number and q always denotes a prime power, thus we use \mathbb{F}_q to denote the field of q elements.

Furthermore, the letters k , m and n (in both the upper and lower cases) denote positive integers.

We recall that the notations $U = O(V)$ and $V \ll U$ are all equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$. The implied constants in the symbols ‘ O ’ and ‘ \ll ’ are absolute.

For a complex z , we define $\mathbf{e}(2\pi iz)$ and $\mathbf{e}_r(z) = \mathbf{e}(z/r)$.

Finally, the notation $z \sim Z$ means that z satisfies the inequalities $Z < z \leq 2Z$.

1.3. Main Result. We extend the definition of $I(t)$ and $\iota(t)$ to arbitrary finite fields of q elements.

Theorem 1.1. *Suppose that R is an integer with*

$$0 < R < 2R < 2\sqrt{q}.$$

We have,

$$\frac{1}{R} \sum_{t \sim R} \iota(t) \ll \frac{\log q}{\sqrt{\log R}} (\log \log q)^{7/2}.$$

In particular, we see from Theorem 1.1 that for any fixed ε there is a constant $c(\varepsilon)$ such that for $R \geq q^\varepsilon$ we have

$$\frac{1}{R} \sum_{t \sim R} \iota(t) \leq c(\varepsilon) (\log q)^{1/2} (\log \log q)^{7/2}.$$

It is also easy to see that it improves on the “individual” bound (1.4) starting with $R \geq (\log \log q)^{3+\varepsilon}$.

2. CHARACTER SUMS AND THE LARGE SIEVE

2.1. Basics on exponential and character sums. We recall, that for any integers z and $r \geq 1$, we have the orthogonality relation

$$(2.1) \quad \sum_{-r/2 \leq b < r/2} \mathbf{e}_r(bz) = \begin{cases} r, & \text{if } z \equiv 0 \pmod{r}, \\ 0, & \text{if } z \not\equiv 0 \pmod{r}, \end{cases}$$

see [5, Section 3.1].

Additionally, we need the bound

$$(2.2) \quad \sum_{n=K+1}^{K+L} \mathbf{e}_r(bn) \ll \min \left\{ L, \frac{r}{|b|} \right\},$$

which holds for any integers b , K and $L \geq 1$ with $0 < |b| \leq r/2$, see [5, Bound (8.6)].

We also refer to [5, Chapter 3] for a background on multiplicative characters.

The link between multiplicative characters and exponential sums is given by the following well-known identity (see [5, Equation (3.12)]) involving Gauss sums

$$\tau_r = \sum_{v=1}^r \chi_r(v) \mathbf{e}_r(v)$$

with the quadratic character χ_r modulo an integer $r \geq 1$, that is, a fully multiplicative function of both argument which coincides with the Legendre symbol if r is an odd prime and also defined for $r = 2$ as

$$\chi_2(v) = \begin{cases} 0, & \text{if } v \equiv 0 \pmod{2}; \\ 1, & \text{if } v \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } v \equiv \pm 3 \pmod{8}. \end{cases}$$

It is easy to see that for any integer v with $\gcd(v, r) = 1$, we have

$$(2.3) \quad \left(\frac{v}{r}\right) \tau_r = \sum_{b=1}^r \left(\frac{b}{r}\right) \mathbf{e}_r(bv).$$

By [5, Lemma 3.1] we also have:

Lemma 2.1. *We have*

$$|\tau_r| \leq r^{1/2}.$$

2.2. Large sieve for quadratic moduli. For $t \in [-T, T]$ we define the function $\Delta(t) = 4q - t^2$.

We make use of the following large sieve type inequality:

Lemma 2.2. *Suppose that $0 < R < 2R < 2\sqrt{q}$. Let $\alpha_1, \dots, \alpha_N$ be an arbitrary sequence of complex numbers and let*

$$Z = \sum_{n=1}^N |\alpha_n|^2 \quad \text{and} \quad \mathcal{T}(x) = \sum_{n=1}^N \alpha_n \mathbf{e}(nx).$$

Then, we have

$$\begin{aligned} & \sum_{t \sim R} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \\ & \leq \left(qR + N + \min \left\{ \sqrt{R}N + \sqrt{q}N^{3/4}, \sqrt{N}q \right\} \right) Z(qN)^{o(1)}. \end{aligned}$$

Proof. Set

$$S = \{\Delta(t) : t \sim R\} = \{\Delta(t) : Q_0 \leq \Delta(t) \leq Q_1\},$$

where $Q_0 = 4q - 4R^2$ and $Q_1 = 4q - R^2$. We start by applying [1, Theorem 2]. Let

$$S_r = \{m \in \mathbb{N} : mr \in S\}.$$

We clearly have $S_r \subseteq [Q_0/r, Q_1/r]$ and S_r is empty unless $4q$ is a square modulo r . Moreover, set

$$A_r(u, k, l) = \max_{Q_0/r \leq y \leq q/r} \#\{m \in S_r \cap (y, y+u] : m \equiv l \pmod{k}\},$$

where $u \geq 0$, $k \in \mathbb{N}$, $l \in \mathbb{Z}$ with $\gcd(k, l) = 1$. Thus $A_r(u, k, l) = 0$ unless the system of congruences

$$\frac{t^2 - 4q}{r} \equiv l \pmod{k}$$

has a solution in t . Following the arguments in [1, Section 6] with minor changes, we get that if $k \leq \sqrt{N}$, then

$$(2.4) \quad A_r(u, k, l) \leq \left(1 + \frac{\#S_r/k}{R^2/r}u\right) N^{o(1)}.$$

Now using [1, Theorem 2] together with a short computation, we get that

$$(2.5) \quad \sum_{\Delta(t) \in S} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \ll \left(N + N^{o(1)}(qR + q\sqrt{N})\right) Z.$$

The remainder of the proof follows closely to those in [1] and [2]. Using [2, Lemma 8], we have the following. Suppose that $0 < D \leq 1/2$ and $\{\beta_l\}$ is a sequence of real numbers such that for all $\alpha \in \mathbb{R}$, there is β_l such that

$$\|\beta_l - \alpha\| \leq D.$$

Then,

$$(2.6) \quad \sum_{\Delta(t) \in S} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \ll K(D)(N + D^{-1})Z,$$

where

$$K(D) = \max_{1 \leq l \leq L} \#\{a/\Delta(t) : \Delta(t) \in S, \gcd(a, \Delta(t)) = 1, \|a/\Delta(t) - \beta_l\| \leq D\}.$$

We choose β_1, \dots, β_L in the same way as in [2] as rationals of the form

$$\beta_l = \frac{b}{r} + \frac{1}{kr^2}, \quad l = 1, \dots, L,$$

with some $b, r \in \mathbb{N}$, $r \leq D^{-1/2}$, $\gcd(b, r) = 1$, $1 \leq b < r$ and $k \in \mathbb{Z}$ with $\lceil r^{-1}D^{-1/2} \rceil \leq |k| \leq \lceil r^{-2}D^{-1} \rceil$. Now let

$$\tau = \frac{1}{\sqrt{D}}, \quad K = \lceil r^{-1}D^{-1/2} \rceil, \quad \kappa = \lceil r^{-2}D^{-1} \rceil,$$

and

$$P(\alpha) = \#\{a/\Delta(t) : \Delta(t) \in S, \gcd(a, \Delta(t)) = 1, |a/\Delta(t) - \alpha| \leq D\}.$$

Using [2, Lemma 9] and the discussion that follows therein, we get that

$$(2.7) \quad K(D) \leq 2 \max_{\substack{r \in \mathbb{N} \\ r \leq \tau}} \max_{\substack{b \in \mathbb{Z} \\ \gcd(b, r) = 1}} \max_{K \leq k \leq \kappa} P\left(\frac{b}{r} + \frac{1}{kr^2}\right).$$

Now set

$$\psi(x) = \left(\frac{\sin \pi x}{2x}\right)^2.$$

Recall that the Fourier transform of ψ is $\hat{\psi}(t) = \max\{0, 1 - |t|\}$ which is compactly supported. We have

$$P(\alpha) \leq \sum_{\Delta(t) \in S} \sum_{a=-\infty}^{\infty} \psi\left(\frac{a - \alpha \Delta(t)}{4qD}\right).$$

Following the same computation as that in [2, Section 4], we get

$$P(\alpha) \ll qRD + qD \sum_{0 < j < (4qD)^{-1}} \left| \sum_{R \leq t \leq 2R} \mathbf{e}(\alpha j t^2) \right|,$$

and then arrive at

$$(2.8) \quad \begin{aligned} & P\left(\frac{b}{r} + \frac{1}{kr^2}\right) \\ & \leq qRD + \left(\frac{R}{\sqrt{r}} + \sqrt{R} + \sqrt{qDr} + \sqrt{RqD}\right) \left(\frac{R}{qD}\right)^{o(1)}. \end{aligned}$$

Next, we now prove an analogue of [2, Equation (5.1)]. Using [1, Lemma 4] and mindful of the bound (2.4), we get

$$(2.9) \quad P\left(\frac{b}{r} + \frac{1}{kr^2}\right) \leq (1 + qDr + qRD) \left(\frac{1}{D}\right)^{o(1)},$$

if $D/2 \leq 1/(kr^2) \leq D$. Now we assume that $1/(kr^2) \geq D$. Very much like in [2, Equation (5.2)], we get

$$\begin{aligned} P\left(\frac{b}{r} + z\right) & \ll 1 + \delta^{-1} \int_{Q_0}^{Q_1} \Omega(\delta, y) dy \\ & \ll 1 + \delta^{-1} \int_{-\infty}^{4q} \exp\left(-\frac{4q-y}{R^2}\right) \Omega(\delta, y) dy, \end{aligned}$$

where

$$\begin{aligned} \Omega(\delta, y) &= \sum_{y-\delta \leq \Delta(t) \leq y+\delta} \sum_{\substack{m \in J(\delta, y) \\ m \equiv -b\Delta(t) \pmod{r} \\ m \neq 0}} 1 \\ &\ll \sum_{t=-\infty}^{\infty} \psi\left(\frac{t - \sqrt{4q - y}}{2c\delta/R}\right) \sum_{\substack{m \neq 0 \\ m \equiv -b\Delta(t) \pmod{r}}} \psi\left(\frac{m - yrz}{8\delta rz}\right), \end{aligned}$$

for some absolute constant c and $J(\delta, y) = [(y-4\delta)rz, (y+4\delta)rz]$. Now applying Poisson summation twice and making a change of variables, we get

$$(2.10) \quad \begin{aligned} P\left(\frac{b}{r} + \frac{1}{kr^2}\right) &\ll \frac{\delta z}{R} \left| \sum_{j=-\infty}^{\infty} \frac{\hat{\psi}(8j\delta z)}{r^*} \mathbf{e}\left(-4qj\left(\frac{b}{r} + z\right)\right) \right. \\ &\quad \left. \sum_{l=-\infty}^{\infty} \hat{\psi}\left(\frac{2cl\delta}{r^*R}\right) G(-j^*b, l; r^*) E(j, l) \right|, \end{aligned}$$

where

$$G(a, l; c) = \sum_{d=1}^c \mathbf{e}\left(\frac{ad^2 + ld}{c}\right)$$

denotes the quadratic Gauss sum with

$$r^* = \frac{r}{(j, r)}, \quad j^* = \frac{j}{(j, r)},$$

and

$$E(j, l) = \int_0^{\infty} \exp\left(-\frac{u}{R^2}\right) \mathbf{e}\left(juz - \frac{l\sqrt{u}}{r^*}\right) du.$$

Note that the upper bound in (2.10) is essentially the same as the right-hand side of [2, Equation (5.3)]. The computations of [2, Sections 7, 8 and 9] go through with minor changes and we arrive at the bound

$$(2.11) \quad P(\alpha) \ll \left(R^{1/2} + RD^{1/4} + R^3D + \sqrt{r} + \frac{RD}{\sqrt{rz}}\right) \left(\frac{R}{D}\right)^{o(1)}.$$

Now combining (2.11) and (2.9) in the same manner as in [2, Sections 10], we derive that

$$(2.12) \quad \begin{aligned} P(\alpha) &\leq \left(\sqrt{R} + RD^{1/4} + qRD + \sqrt{r} + \sqrt{qRD}r^{1/4} + qDr\right) \\ &\quad \left(\frac{q}{D}\right)^{o(1)}. \end{aligned}$$

Now recall that $r \leq D^{-1/2}$. We use (2.8) if $r > R$ and (2.12) if $r \leq R$, we get

$$P(\alpha) \leq \left(qRD + \sqrt{R} + \sqrt{q}D^{1/4} + \sqrt{q}R^{3/4}D^{1/2} \right) \left(\frac{q}{D} \right)^{o(1)}.$$

Setting $D = 1/N$ and applying the above bound to (2.7) and then to (2.6), we get

$$\begin{aligned} \sum_{t \sim R} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \\ \leq \left(qR + \sqrt{R}N + \sqrt{q}N^{3/4} + \sqrt{q}R^{3/4}N^{1/2} \right) Z(qN)^{o(1)}. \end{aligned}$$

Now if $N \leq q\sqrt{R}$, then

$$\sqrt{q}R^{3/4}N^{1/2} \leq qR.$$

If $N > q\sqrt{R}$, then

$$\sqrt{q}R^{3/4}N^{1/2} \leq \sqrt{RN}.$$

Hence

$$\begin{aligned} (2.13) \quad \sum_{t \sim R} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \\ \leq \left(qR + \sqrt{R}N + \sqrt{q}N^{3/4} \right) Z(qN)^{o(1)}. \end{aligned}$$

The desired result follows by comparing the above to (2.5). \square

2.3. Multiple divisor function. For positive integers k , M and ν we denote by $d_{\nu}(k, M)$ the number of integer factorisations of k of the form

$$k = m_1 \dots m_{\nu}, \quad \text{with } 1 \leq m_1, \dots, m_{\nu} \leq M.$$

We need the following bound, uniform with respect to all parameters which is due to Garaev [4, Lemma 8].

Lemma 2.3. *We have*

$$\sum_{k \leq M^{\nu}} d_{\nu, M}(k)^2 \leq M^{\nu} \left(\frac{e \log M}{\nu} + e \right)^{\nu^2}.$$

2.4. Bound of character sums on average. Let ξ_t be the quadratic character modulo $\Delta(t)$ (as defined in Section 2.1). We consider the character sums

$$S_t(N) = \sum_{n=1}^N \xi_t(n).$$

We follow the ideas of Garaev [4, Theorem 3] to obtain the following result. Throughout this section, we define

$$(2.14) \quad X = \max \left\{ q\sqrt{R}, \frac{q^2}{R^2} \right\}.$$

Lemma 2.4. *Suppose that R is an integer with $0 < R < 2R < 2\sqrt{q}$. For positive integer L and ν , such that*

$$(2.15) \quad L^\nu \geq X$$

we have

$$\sum_{t \sim R} \max_{N \sim L} |S_t(N)| \leq R^{1-1/(4\nu)} L^{1+o(1)} \left(\frac{e \log(2L)}{\nu} + e \right)^{\nu/2},$$

as $L \rightarrow \infty$.

Proof. For each integer $t \in [-T, T]$ we choose $N_t \sim L$, with

$$|S_t(N_t)| = \max_{N \sim L} |S_t(N)|.$$

Let $M = 2L$. Using (2.1), for $N_t \sim L$ we write

$$\begin{aligned} \sum_{n=1}^{N_t} \xi_t(n) &= \sum_{m=1}^M \xi_t(m) \frac{1}{M} \sum_{n=1}^{N_t} \sum_{b=-L}^{L-1} \mathbf{e}_M(b(m-n)) \\ &= \frac{1}{M} \sum_{b=-L}^{L-1} \sum_{n=1}^{N_t} \mathbf{e}_M(-bn) \sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm). \end{aligned}$$

Recalling (2.2), we derive

$$\left| \sum_{n=1}^{N_t} \xi_t(n) \right| \ll \sum_{b=-L}^{L-1} \frac{1}{|b|+1} \left| \sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right|.$$

Therefore,

$$(2.16) \quad \sum_{t \sim R} \max_{N \sim L} |S_t(N)| = \sum_{t \sim R} \left| \sum_{n=1}^{N_t} \xi_t(n) \right| \ll \sum_{b=-L}^{L-1} \frac{1}{|b|+1} W_b$$

where

$$W_b = \sum_{t \sim R} \left| \sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right|.$$

By Hölder's inequality, we get the bound

$$W_b^{2\nu} \leq R^{2\nu-1} \sum_{t \sim R} \left| \sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right|^{2\nu}.$$

We now note that

$$\left(\sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right)^\nu = \sum_{k=1}^K \rho_{b,\nu}(k) \xi_t(k),$$

where $K = M^\nu$ and

$$\rho_{b,\nu}(k) = \sum_{\substack{m_1, \dots, m_\nu=1 \\ m_1 \dots m_\nu = k}}^M \mathbf{e}_M(b(m_1 + \dots + m_\nu)).$$

Using (2.3), we write

$$\left(\sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right)^\nu = \sum_{k=1}^K \rho_{b,\nu}(k) \frac{1}{\tau_t} \sum_{v=1}^{\Delta(t)} \xi_t(v) \mathbf{e}_{\Delta(t)}(kv).$$

Changing the order of summation, by Lemma 2.1 and the Cauchy inequality, we obtain,

$$\left| \sum_{m=1}^M \xi_t(m) \mathbf{e}_M(bm) \right|^{2\nu} \leq \sum_{v=1}^{\Delta(t)} \left| \sum_{k=1}^K \rho_{b,\nu}(k) \mathbf{e}_{\Delta(t)}(kv) \right|^2.$$

Thus,

$$W_b^{2\nu} \leq R^{2\nu-1} \sum_{t \sim R} \sum_{\substack{v=1 \\ \gcd(v, \Delta(t))=1}}^{\Delta(t)} \left| \sum_{k=1}^K \rho_{b,\nu}(k) \mathbf{e}_{\Delta(t)}(kv) \right|^2$$

Using that $|\rho_{b,\nu}(k)| \leq d_{\nu,M}(k)$ and recalling Lemma 2.3, we now derive from Lemma 2.2, estimating Z as

$$Z \ll M^\nu \left(\frac{e \log M}{\nu} + e \right)^{\nu^2},$$

that

$$W_b^{2\nu} \leq R^{2\nu-1} M^\nu \left(\frac{e \log M}{\nu} + e \right)^{\nu^2} \left(qR + M^\nu + \min \left\{ \sqrt{R} M^\nu + \sqrt{q} M^{3\nu/4}, M^{\nu/2} q \right\} \right) (M^\nu q)^{o(1)}.$$

Always using the first term in the above minimum, we obtain

$$W_b^{2\nu} \leq R^{2\nu-1} M^\nu \left(\frac{e \log M}{\nu} + e \right)^{\nu^2} \left(qR + \sqrt{R}M^\nu + \sqrt{q}M^{3\nu/4} \right) (M^\nu q)^{o(1)}.$$

Mindful of the inequality $L^\nu \geq \max\{q\sqrt{R}, q^2/R^2\}$, we see that in the above inequality, the term $\sqrt{R}M^\nu$ dominates over $qR + \sqrt{q}M^{3\nu/4}$. So the last display simplifies further as

$$W_b^{2\nu} \leq R^{2\nu-1/2} M^{(2+o(1))\nu} \left(\frac{e \log M}{\nu} + e \right)^{\nu^2}.$$

Therefore

$$W_b \leq R^{1-1/(4\nu)} L^{1+o(1)} \left(\frac{e \log(2L)}{\nu} + e \right)^{\nu/2}.$$

Inserting this into (2.16), we conclude the proof. \square

We remark here that simply using the classical large sieve inequality, the sum in Lemma 2.2 is

$$\sum_{t \sim R} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \leq (q^2 + N)Z.$$

Using this bound, one can still arrive at a non-trivial estimate in Lemma 2.4, but the condition in (2.15) needs to be replaced by $L^\nu > q^2$. Moreover, as in [8], we can conjecture that

$$\sum_{t \sim R} \sum_{\substack{a=1 \\ \gcd(a, \Delta(t))=1}}^{\Delta(t)} |\mathcal{T}(a/\Delta(t))|^2 \leq (qR + N)(qN)^{o(1)}Z.$$

Having this bound at one's disposal, a non-trivial bound in Lemma 2.4 can be obtained as soon as $L^\nu > qR$.

We now obtain a bound on character sums $S_t(N)$ on average starting from rather short intervals of length $N \sim L$ with

$$(2.17) \quad \frac{\log L}{\sqrt{\log \log L}} \geq \frac{4 \log X}{\sqrt{\log R}},$$

where, as before, X is given by (2.14).

Corollary 2.5. *Suppose that R is an integer with $0 < R < 2R < 2\sqrt{q}$. For all integers L satisfying (2.17), we have*

$$\sum_{t \sim R} \max_{N \sim L} |S_t(N)| \leq RL \exp \left(-(7/8 + o(1)) \sqrt{\log R \log \log L} \right)$$

as $L \rightarrow \infty$.

Proof. We assume that L is sufficiently large and choose

$$\nu = \left\lceil \frac{1}{4} \sqrt{\frac{\log R}{\log \log L}} \right\rceil + 3.$$

We see from (2.17) that

$$\nu \log L \geq 4\nu \log X \sqrt{\frac{\log \log L}{\log R}} \geq \log X,$$

and thus Lemma 2.4 is applicable with this parameter ν . Furthermore

$$\begin{aligned} \left(\frac{e \log(2L)}{\nu} + e \right)^{\nu/2} &\leq (\log(2L) + e)^{\nu/2} \\ &= \exp((1/2 + o(1))\nu \log \log(2L)) \\ &= \exp\left((1/8 + o(1))\sqrt{\log R \log \log L}\right). \end{aligned}$$

We also have

$$R^{1/4\nu} = \exp\left(\frac{1}{4\nu} \log R\right) = \exp\left((1 + o(1))\sqrt{\log R \log \log L}\right).$$

Thus recalling Lemma 2.4, we conclude the proof. \square

3. PROOF OF THEOREM 1.1

3.1. Isogeny classes and L -functions. Let $\mathcal{L}(t) = L(1, \chi_t)$ be the value of the L -function at $s = 1$ which correspond to the quadratic character modulo $\Delta_t = 4p - t^2$ and let $\mathcal{L}^*(t) = L(1, \chi_t^*)$ be the value of the L -function at $s = 1$ which corresponds to the quadratic character modulo $\Delta_t^* = \Delta_t / f_t^2$ where f is the largest integer such that $f^2 \mid \Delta$ and $\Delta_0 \equiv 0, 1 \pmod{4}$.

We need the following two results which follow from the identities and estimates given by Lenstra [6, Pages 654–656]. We obtain the following two relations. First we have

$$(3.1) \quad I(t) = \frac{\sqrt{\Delta_t}}{2\pi} \mathcal{L}^*(t) \psi(f_t)$$

where $\psi(f)$ is an explicitly defined function which for an integer $f \geq 1$ satisfies the bound

$$(3.2) \quad \psi(f) \ll (\log \log(f+2))^2.$$

Then, we also have

$$(3.3) \quad \mathcal{L}(t) = \mathcal{L}^*(t) \prod_{\substack{\ell|f \\ \ell \text{ prime}}} \left(1 - \frac{\chi_t^*(\ell)}{\ell}\right),$$

(which follows from the Dirichlet product formula for L -functions).

Clearly,

$$\prod_{\substack{\ell|f \\ \ell \text{ prime}}} \left(1 - \frac{\chi_t^*(\ell)}{\ell}\right)^{-1} \leq \prod_{\substack{\ell|f \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell}\right)^{-1}$$

Using the fact that f has at most $O(\log f)$ prime factors and recalling the Mertens formula, see [5, Equation (2.16)], we obtain

$$\prod_{\substack{\ell|f \\ \ell \text{ prime}}} \left(1 - \frac{\chi_t^*(\ell)}{\ell}\right)^{-1} \ll \log \log(f+2).$$

Hence, collecting (3.1), (3.2) and (3.3) together we obtain

Lemma 3.1. *We have,*

$$I(t) \ll \sqrt{\Delta_t} \mathcal{L}(t) (\log \log q)^3.$$

We remark that with a little bit of care, one can be more precise with the double logarithmic function in Lemma 3.1. However, to streamline the exposition, we ignore this minor savings and concentrate on the powers of $\log q$.

3.2. Bounds of L -functions. We now give a bound on the average value of $\mathcal{L}(t)$ over dyadic intervals.

Lemma 3.2. *Suppose that R is an integer with*

$$(\log q)^2 < R < 2R < 2\sqrt{q}.$$

Then we have

$$\sum_{t \sim R} |\mathcal{L}(t)| \ll \log q \sqrt{\frac{\log \log q}{\log R}}$$

as $R \rightarrow \infty$.

Proof. Let X be defined by (2.14). We write $L_j = 2^j$ for $j = J, J + 1, \dots$, where J is defined by the inequalities

$$\frac{\log 2^{J-1}}{\sqrt{\log \log 2^{J-1}}} < \frac{4 \log X}{\sqrt{\log R}} \leq \frac{\log 2^J}{\sqrt{\log \log 2^J}}.$$

Thus we can apply Corollary 2.5 with $L = L_j$ for any $j \geq J$.

We also define I by the conditions

$$2^{I-1} \leq q^2 < 2^I$$

Since for any integer $N \geq 1$, we trivially have

$$\left| \sum_{n=1}^N \xi_t(n) \right| \leq \Delta_t \leq q$$

By partial summation, we immediately obtain

$$(3.4) \quad \sum_{n \geq L_I} \frac{\xi_t(n)}{n} \ll 1.$$

For $J \leq j \leq I$, invoking Corollary 2.5 and using partial summation again, we derive

$$\sum_{t \sim R} \left| \sum_{L_j \leq n < L_{j+1}} \frac{\xi_t(n)}{n} \right| \leq R \exp \left(-(7/8 + o(1)) \sqrt{\log R \log j} \right).$$

Hence

$$\begin{aligned} \frac{1}{R} \sum_{t \sim R} \left| \sum_{L_J \leq n \leq L_I} \frac{\xi_t(n)}{n} \right| &\ll \sum_{J \leq j \leq I} \exp \left(-(7/8 + o(1)) \sqrt{\log R \log j} \right) \\ &\leq \sum_{2 \leq j \leq I} \exp \left(-(7/8 + o(1)) \sqrt{\log R \log j} \right) \\ &\leq \sum_{h=0}^H \exp \left(h - (7/8 + o(1)) \sqrt{h \log R} \right), \end{aligned}$$

where $H = \lfloor \log I \rfloor$. Since $I \sim 2 \log q$ we have $H \sim \log \log q$. Thus for $\log R > 2 \log \log q$ and $h \leq H$, we see that

$$\frac{7}{8} \sqrt{h \log R} \geq \frac{7\sqrt{2}}{8} h > \frac{6h}{5}$$

and we obtain

$$(3.5) \quad \begin{aligned} \frac{1}{R} \sum_{t \sim R} \left| \sum_{L_J \leq n \leq L_I} \frac{\xi_t(n)}{n} \right| &\leq \sum_{h=0}^H \exp \left(h - (7/8 + o(1)) \sqrt{h \log R} \right) \\ &\leq \sum_{h=0}^H \exp \left(-(1/5 + o(1))h \right) \ll 1. \end{aligned}$$

Finally we also use the trivial bound

$$(3.6) \quad \sum_{n < L_J} \frac{\xi_t(n)}{n} \ll \log L_J \ll \log X \sqrt{\frac{\log \log X}{\log R}}.$$

Combining (3.4), (3.5), and (3.6), and using that $q \leq X \leq q^2$, we conclude the proof. \square

3.3. Concluding the proof. We observe that for $R \leq (\log q)^2$ the result follows immediately from (1.4) (which can be extended to arbitrary fields without any changes in the argument).

Otherwise we combine Lemmas 3.1 and 3.2 to derive the desired estimate.

REFERENCES

- [1] S. Baier, ‘On the large sieve with sparse sets of moduli’, *J. Ramanujan Math. Soc.*, **21** (2006), 279–295.
- [2] S. Baier and L. Zhao, ‘An improvement for the large sieve for square moduli’, *J. Number Theory*, **128** (2008), 154–174.
- [3] B. J. Birch, ‘How the number of points of an elliptic curve over a fixed prime field varies’, *J. Lond. Math. Soc.* **43** (1968), 57–60.
- [4] M. Z. Garaev, ‘Character sums in short intervals and the multiplication table modulo a large prime’, *Monat. Math.*, **148** (2006), 127–138.
- [5] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.
- [6] H. W. Lenstra, ‘Factoring integers with elliptic curves’, *Annals of Math.*, **126** (1987), 649–673.
- [7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 2009.
- [8] L. Zhao, ‘Large sieve inequality for characters to square moduli’, *Acta Arith.*, **112** (2004), 297–308.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,
SYDNEY, NSW 2052, AUSTRALIA

E-mail address: igor.shparlinski@unsw.edu.au

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,
SYDNEY, NSW 2052, AUSTRALIA

E-mail address: l.zhao@unsw.edu.au